REMARKS

Enclosed herewith is a Substitute Specification in which the specification as filed has been amended in various places to correct typographical and grammatical errors, and to also add section headings. The specification has also been amended to cite U.S. Patents 5,943,422 and 6,157,721 corresponding to International Patent Application No. WO 97/43761 cited on page 3 of the specification as filed. Enclosed herewith is form PTO/SB/08A listing these U.S. patents.

In support of the above, enclosed herewith is a copy of the specification as filed marked up with the above changes.

The undersigned attorney asserts that no new matter has been incorporated into the Substitute Specification.

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, the claims have been amended for clarity.

Applicants believe that the above changes answer the Examiner's objection to claims 10 and 11 under 37 C.F.R. 1.75(a), and respectfully request withdrawal thereof.

The Examiner has rejected claims 1 and 3-13 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0042043 to Shear et al. in view of U.S. Patent 6,226,618 to Downs et al. and U.S. Patent 5,892,900 to Ginter et al. The Examiner has further rejected claim 2 under 35 U.S.C.

103(a) as being unpatentable over Shear et al. in view of Downs et al. and Ginter et al., and further in view of U.S. Patent 6,064,751 to Smithies et al.

The Shear et al. publication discloses cryptographic methods, apparatus and systems for storage media electronic rights management in closed and connected appliances, in which digital information 200, metadata 202 and associated controls 204 are stored on a storage medium 100, and that a key block 208 containing one or more cryptographic keys for decrypting the digital information 200 and the metadata 202. The key block 208 may itself be encrypted by hidden keys 210 stored in a location on the storage medium 100 not normally accessible.

The Downs et al. patent discloses an electronic content delivery system, in which an end-user device 109 includes player application 195 for scrambling the content 113 on receipt and marks the content 113 with a copy/play code 523 representing the initial copy/play permission. The player application 195 generates a scrambling key for each of the received content 113, encrypts the scrambling keys and stores them in a hidden place in the end-user device 109. Then, each time the end-user device 109 accesses the content 113, the end-user device 109 verifies the copy/play code 523 before allowing descrambling of the content 113, and also updates the copy/play code of the content 113.

The Ginter et al. patent discloses systems and methods for secure transaction management and electronic rights protection, in which the one or more keys used to encrypt each permission record 808 or other management information record will be changed every time the record is updated.

Applicants submit that while Shear et al. discloses encrypting the digital work with an encryption key, and that the encryption key may be encrypted by a hidden key, Shear et al. neither discloses or suggests that the control should be encrypted by a hidden information.

With regard to Downs et al. Applicants submit that the digital work (content 113) is stored with in the end-user device which can actively deny a user to access and modify the usage right, e.g., by storing such information deeply inside an integrated circuit. Applicants believe that Downs et al. is not relevant to the subject invention which claims a passive record carrier storing the information on a surface which is open for inspection.

Applicants submit that as with Downs et al., Ginter et al. stores the usage rights, i.e., the permission records with a device (see col. 136, lines 23-28). While Ginter et al. indicates, at col. 212, lines 43-52, that an encryption key should be periodically changed in order to lessen the time during which each key is used, giving an attacker less ciphertext to use in an attempt to obtain

the key, Applicants urge that this is irrelevant to the subject invention. What matters, in the subject invention, is that the usage rights (a small quantity of ciphertext) are re-encrypted after each change, where the encryption key is managed in such a way that it does not help an attacker to overwrite a newer version or the encrypted usage rights with an older version, in an attempt to undo consumption of one or more rights.

Applicants therefore believe that a record carrier, as claimed, is substantially different from an active device. Most notably, a typical passive record carrier is vulnerable against a "copy and restore" attack, which is explained in the Substitute Specification on page 5, line 20 to page 6, line 7 (paragraph [0012]), whereas an active device has no such vulnerability.

The Smithies et al. patent discloses a document and signature data capture system and method, in which, before encryption, "the contents of the signature envelope 10, together wit ha key provided by the client application 2, are checksummed using the same technique as is used for checksumming the file. Without knowledge of the key used by the original client application 2 when it caused the signature envelope 10 to be built, it would therefore be impractical to modify the signature envelope 10 and regenerate a satisfactory checksum."

However, Applicants submit that Smitbies et al. does not supply that which is missing from Shear et al., Downs et al. and

Ginter et al., i.e., a record carrier storing a digital work and usage right information, in which the usage right information is updated with every use of the digital work, and that a hidden information stored in a hidden channel of the record carrier and used to encrypt or verify the usage right information, is changed when the usage right information is changed.

In view of the above, Applicants believe that the subject invention, as claimed, is not rendered obvious by the prior art, either individually or collectively, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-13, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by _____
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as First-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

On August 15, 2005

By Bennett James